State of Maryland

Department of Budget and Management

Introduction to Digital Evidence Seizure

Target: Network / Technical Response Administrators

September 2003

Presenting Agency
Maryland State Police, Information Technology Bureau
Technical Investigation Division, Computer Forensic Laboratory

What Matters

One Hundred years from now,
It will not matter
What kind of car I drove
What kind of house I lived in,
How much I had in my bank account,
Nor what my clothes looked like,

But the World may be a little better
Because I was important
In the life of a child.

(Author Unknown)

Almost all Computer Crimes Units start from federally funded grants that aim at protecting children. Once CCUs are established they can expand the scope of their expertise. Since the Patriot Act The US Government has expanded the distribution of funds to Establish CCUs aimed at fighting terrorism.

Agenda

TID Mission Statement

TID Organization and Functions

How Computers are used in Crimes

Personal Statistics

Who, What, When , Where crimes occur

Magnitude of Information

Hard Disk Anatomy

About Data Storage

Forensic SOP

Forensic Process

Q&A

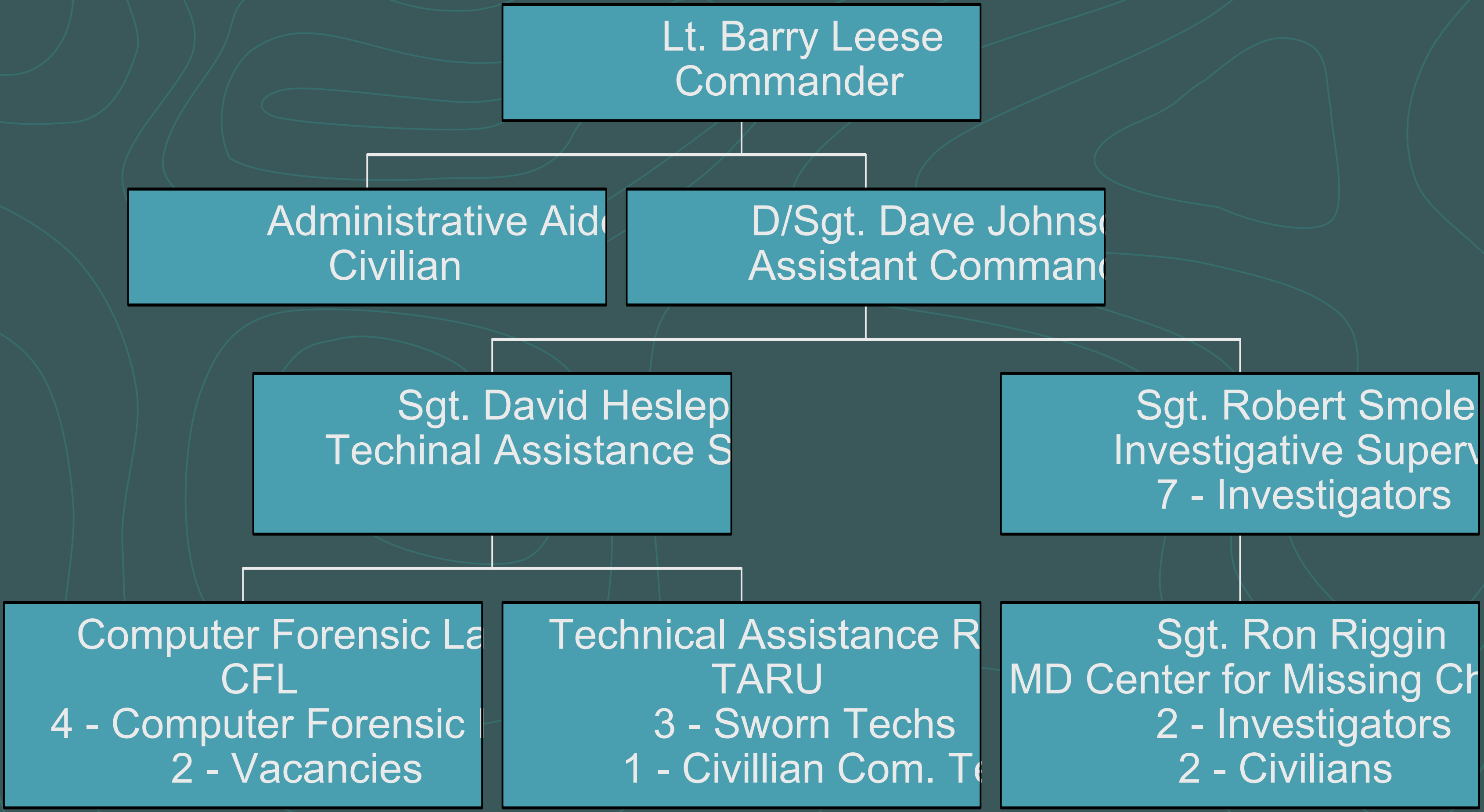
Mission Statement

"The primary mission of the Maryland State Police Computer Crimes Unit, Computer Forensic Laboratory is to provide computer forensic resources to the Computer Crimes Unit and the Internet Crimes Against Children Task Force. In addition, these resources are also provided to Maryland State Police Installations and any other federal, state or local agency that requests this service in support of a **criminal investigation**."

COMPUTER CRIMES

MARYLAND STATE POLICE

Technical Investigation Division



Lt. Barry Leese
Commander

Administrative Aid
Civilian

D/Sgt. Dave Johns
Assistant Comman

Sgt. David Heslep
Techinal Assistance S

Sgt. Robert Smole
Investigative Superv
7 - Investigators

Computer Forensic La
CFL
4 - Computer Forensic
2 - Vacancies

Technical Assistance R
TARU
3 - Sworn Techs
1 - Civillian Com. Te

Sgt. Ron Riggin
MD Center for Missing Ch
2 - Investigators
2 - Civilians

Technical Investigation Division

Core Competencies

Investigative:

- Child Exploitation
- Fraud
- Identity Theft
- Network Intrusion
- Child Vice and Online Prostitution
- Missing Children
- Teaching

Technical:

- Computer Forensics
- Technical Surveillance
- Wiretap (Title III)
- Assisting Other PD
- Onsite Imaging
- Video Enhancement
- Teaching

Corporal Antonio G. Rosela, Jr

Assistant Computer Forensic Laboratory Supervisor

Assignment History

- July 1997 - Appointed to the MSP Academy
- January 1998 - Assigned - Prince Frederick Barrack
- January 1999 - Assigned - Glen Burnie Barrack
- September 2000 - Assigned - Attorney Generals Office - Environmental Crimes Unit
- August 2001 - Assigned - Computer Crimes Unit Computer Forensic Laboratory
- October 2001 - Assigned as Assistant Laboratory Supervisor.

Computer Forensic Stats

Since assignment to February 4, 2003

Completed Examinations: 153

Forensic Hours: 2,450

Data Examined MB: 1,086,668

Data Examined TB: 1.036

Operating Systems: Windows (All Flavors), Macintosh (All Flavors), Red Hat Linux.

File Systems: FAT 12, 16, 32, HFS, HFS+, Joliet, AIFF, Memory Stick, Compact Flash, Smart Media.

Types of Cases: Internal, Administrative, Child Abuse, Sexual Child Abuse, Child Solicitation, Child Pornography, Rape, Murder, Murder for Hire, Theft, CDS, Terrorism, Firearms, Critically Missing Children, Theft, Identity Theft, Fraud, Manufacturing False Documents, Stalking, Email Harassment and Network Intrusion.

Supplemental Duties

- Day-to-Day Laboratory Operations and Management
- New CFI Training
- Course Development and Presentations
- Equipment Evaluation and Testing
- Software Evaluation and Testing
- Assist and Consult for WAN/LAN design, security and deployment for the Agency throughout the State
- Coordinate and Execute Search and Seizure Warrants throughout the State

Why are computers used in crime?

Anonymity (at least some people think so.)

Ease of use, greatly expands the realm to those who would not have otherwise thought of committing crime.

Time to commit crime is not the same as traditional crimes:

Hours of Darkness

Opportunity

Location

Targets (people)

It's always time to commit a computer crime.

Computers in the Criminal World

Computers have become an integral tool within our daily lives, with this has come the ever increasing use of computers and digital media in criminal activity.

Computers can be used three ways during the commission of a crime:

(1) contraband,

(2) fruits of the crime, tool of the offense, or

(3) a storage container holding the evidence of the offense.

Crime Timeline

When are people most likely to commit crimes using the computer?

Early in the day

At lunchtime

After hours

Using remote access

During a time when the supervisor is not around

Reality = Anytime

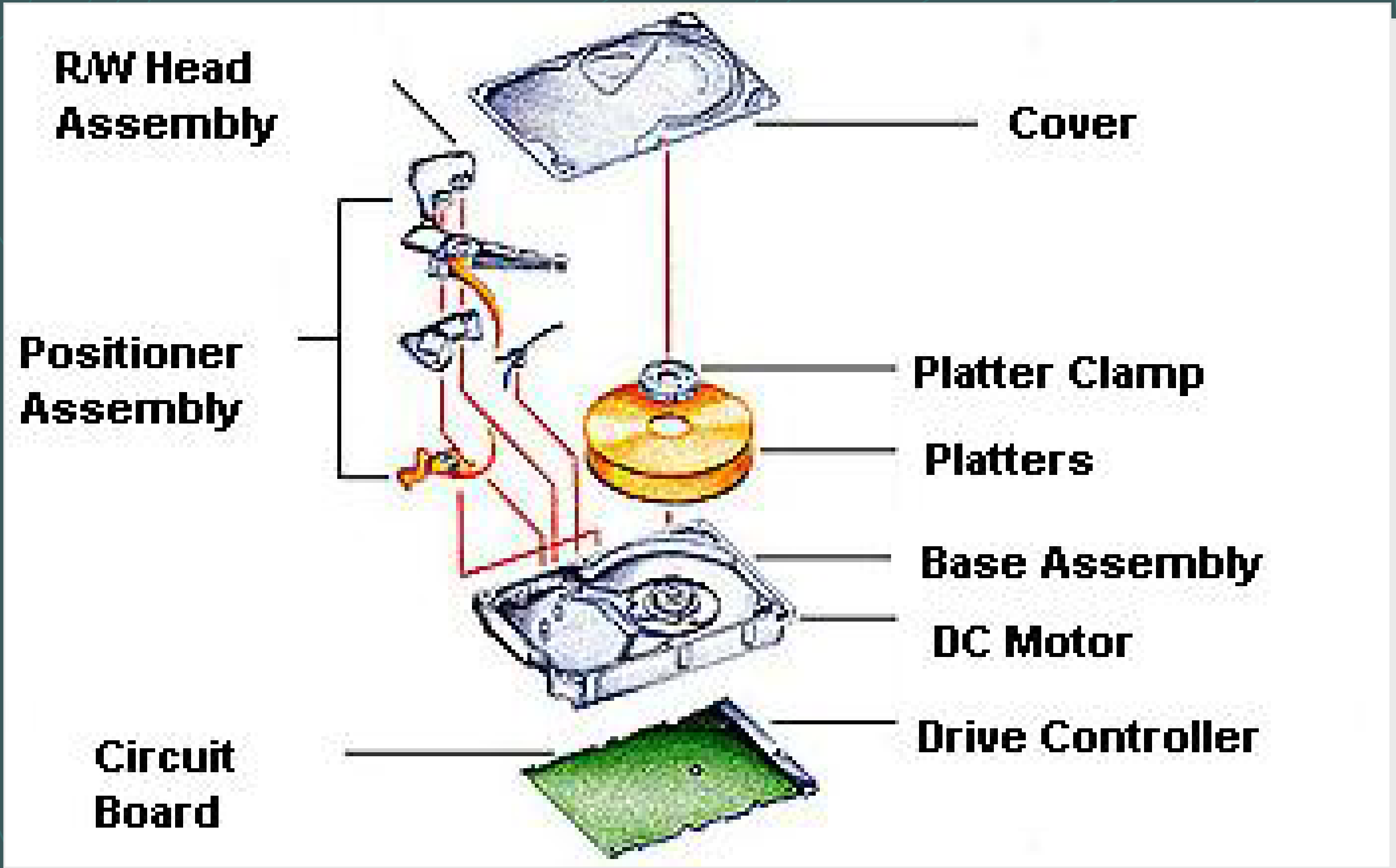
Magnitude of Information

- 1 byte = 8 bits = single character
- 1 kilobyte (KB) = 1024 bytes = paragraph
- 1 megabyte (MB)= 1024 kb = 1,048,576 bytes
  small paperback novel
- 1 gigabyte (GB) = 1024 MB = 1,048,576 (KB) = 1,073,741,824 bytes
  30 feet + of shelved books.
- 1 terabyte (TB)= 1024 GB = 1,048,576 MB
  50,000 trees made into paper and printed
- 1 petabyte = 1024 TB = printed papers of every US research library currently used
- 1 exabyte (EB) = 1024 PB = 5 exabytes
  all words ever spoken by humans from ~5000 BC to present.

Hard Disks

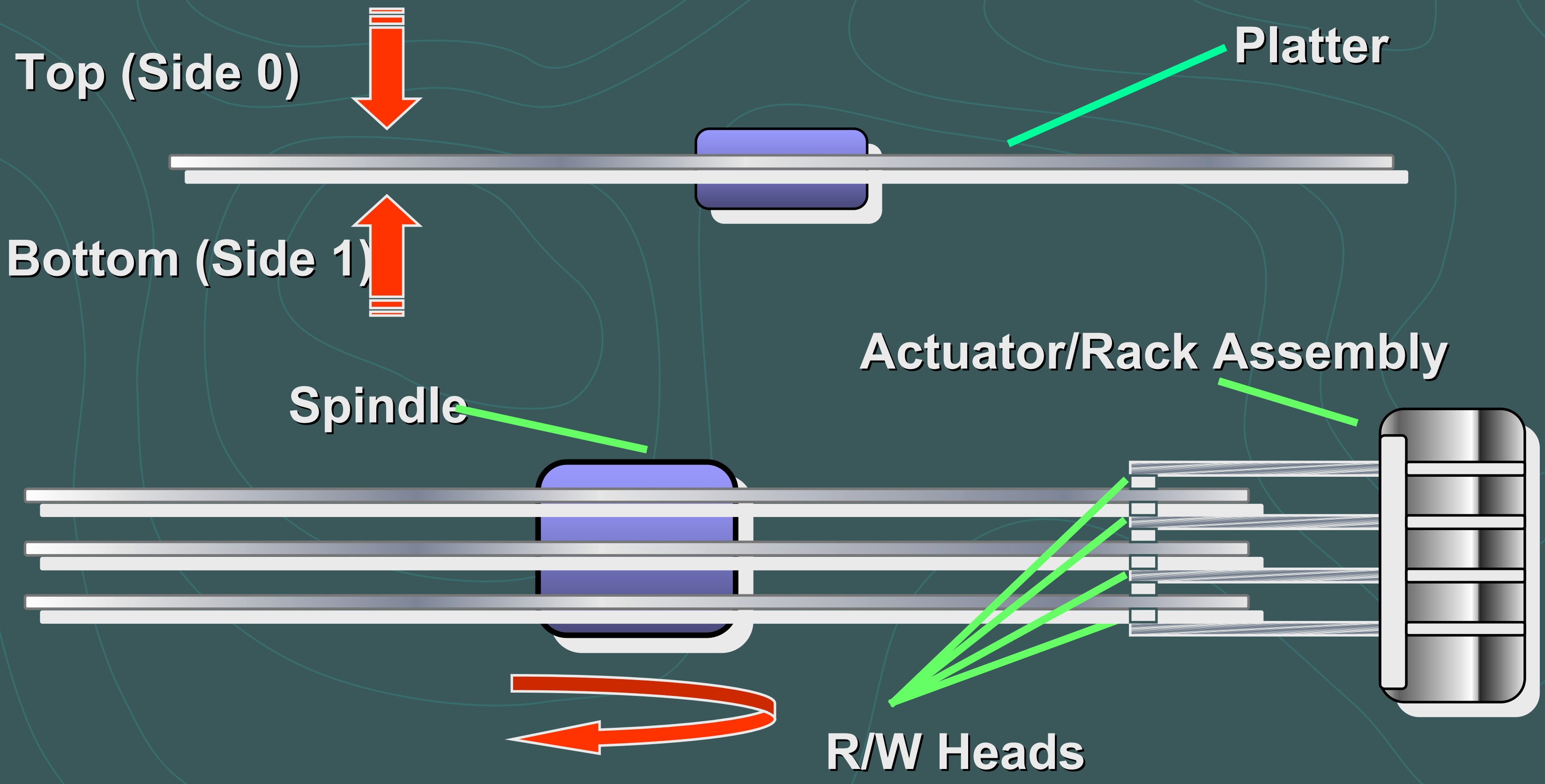
- Generally, the primary data storage device
- One computer may contain multiple physical hard disks that can be partitioned into several logical volumes.
- Many manufacturers: IBM, Maxtor, Seagate, Western Digital and others.

Hard Disk Anatomy



Head Assembly

Side Views



Top (Side 0)

Platter

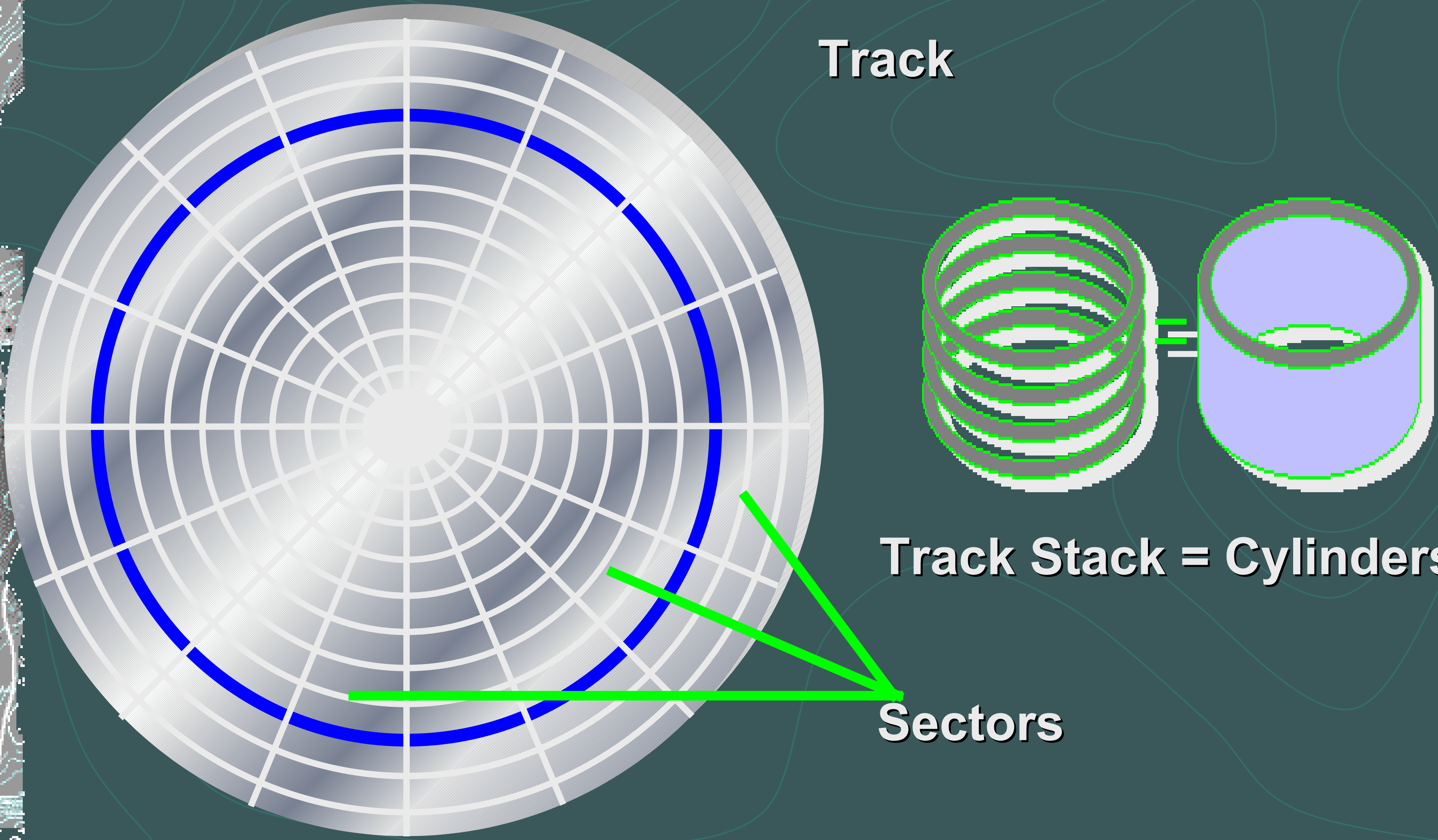
Bottom (Side 1)

Actuator/Rack Assembly

Spindle

R/W Heads

Hard Disk Addressing

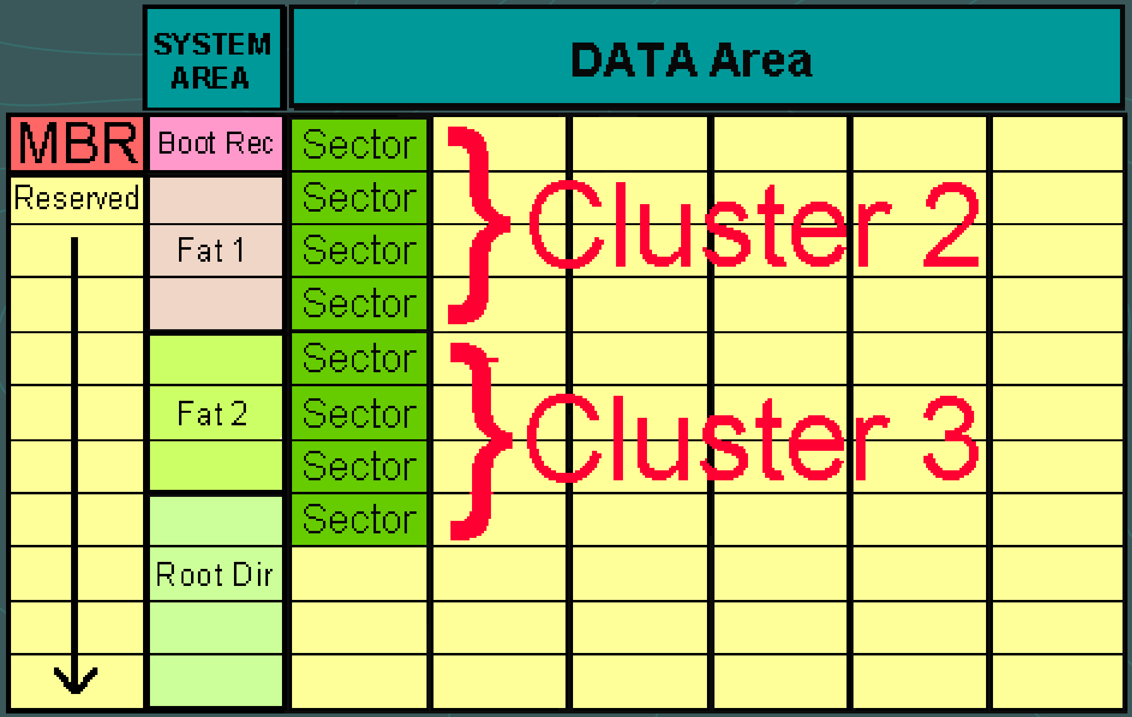


Track

Track Stack = Cylinders

Sectors

Hard Disk Layout



SYSTEM AREA

DATA Area

MBR

Reserved

Boot Rec

Fat 1

Fat 2

Root Dir

Sector

Sector

Sector

Sector

Sector

Sector

Sector

Sector

Cluster 2

Cluster 3

How Computers Store Data

A **Sector** is a continuous linear stream of magnetized Bits and occupies a curved section of a track.

Sectors are the smallest **physical** storage units on a disk and store 512 bytes of data.

Sector numbering starts with 0.

Anatomy of a Sector

The sector "preamble" is written during formatting:

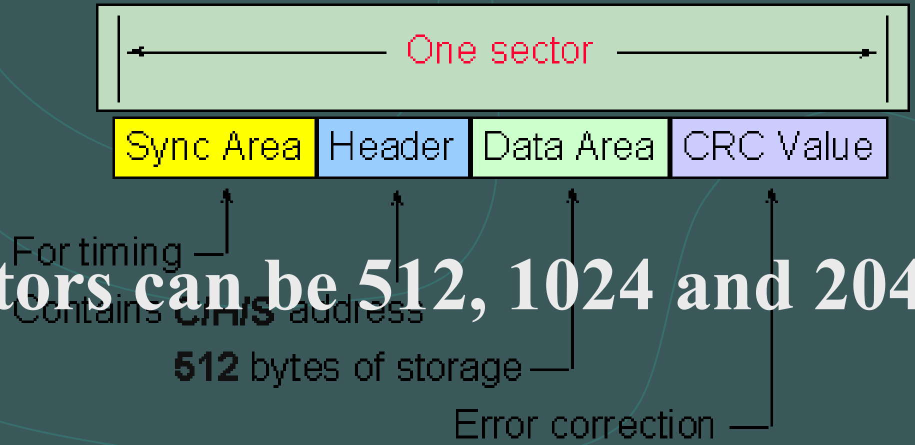
Synchronization bytes - Sector address

If the preamble is corrupt the error "Sector Not Found" is given.

After the data area, there is a section for an error-checking algorithm.

DOS Format

One Sector = 512 bytes



One sector

Sync Area | Header | Data Area | CRC Value

For timing

Contains C/H/S address

512 bytes of storage

Error correction

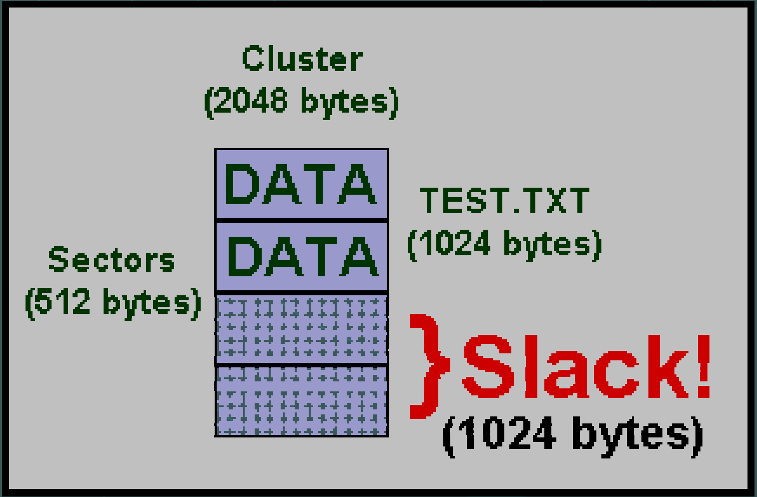
Sectors can be 512, 1024 and 2048 bytes

File Slack

File slack is that space between the end of the file and the end of the cluster.

Four sectors = one cluster.

It COULD contain evidence!



RAM Slack

Before data is written to disk it must fill a sector. The space between the end of the data and the end of the sector is written with data from the RAM. Therefore, information that was never intentionally meant to be saved can be found in the RAM Slack. After Windows 98 RAM Slack was “zeroed” prior to writing to sector.

Other Free Space

- Unallocated space
  - Information not written in the FAT
  - Contains some Internet and chat content.
  - Thorough searching often reveals deleted data, chat conversations and images.

Deleted Files

Just because you delete a file does not mean that the data is gone.

Deleting a file is like taking the index page out of a book without removing the page(s) containing the data.

Once a file is deleted all of the content is still on the disk, the file space is just listed as unallocated until such time as the computer overwrites the data with another file.

Computer Forensic SOP’s

Writing Computer Forensic SOP’s is difficult due to
the following:

Technology is rapidly changing, making standardizing protocols extremely hard.

Every computer crime case is different, looking for different Types of data.

There are no Federal SOP Guidelines to pull from.

Handling Digital Evidence

Cardinal Rules of Computer Forensics

1. NEVER WORK ON ORIGINAL EVIDENCE!
2. Never Mishandle Evidence
3. Never Trust Suspect’s OS
4. Document Everything

Imaging

Generally imaged on stand-alone non-networked computers.

Imaging Starts with a Control Boot on the stand alone to make sure the computer is working correctly.

There are no hard disks attached to the computer during the initial control boot.

The second control boot has the Forensic hard disk, or other forensic recording media, attached to the system to make sure it is correctly recognized.

The final control boot contains both the suspect and Forensic hard disks.

Initiation of the Imaging application is conducted and the suspect drive is imaged to a forensic disk or other forensic media.

Imaging suspect hard disks varies depending upon imaging software, CPU speed, size of drive and verification process (hash or CRC).

Imaging Software

Safeback

Widely used in the Forensic Community.

Performs Imaging, Verification and Restoration Features only.

Currently supports Hard Drive to Hard Drive and SCSI port connections.

EnCase

DOS or Windows Based Evidence Acquisition.

Currently supports Hard Drive to Hard Drive, USB Mass Storage Devices, Parallel Laplink, and SCSI port connections.

Norton Ghost

Snapback

Processing Notes

Start detailed note taking from the crime scene. Include connectivity to computer (printer, modem line, input devices, speakers, monitor).

Describe and sketch room computer will be seized from.

Take accurate notes during imaging and examination.

Examination software suites such as EnCase and I-Look will record certain aspects of the examination, such as: Type and Size of Media being examined and Time, Date and Results of Keyword Text String Searches.

Validation of Evidence

Cyclical Redundancy Checksum (CRC)

- CRC is used to verify the integrity of each block of data. Odds of two different blocks having the same CRC is approximately 1 in 4 billion.

- Most hard drives store one CRC for every sector (512 bytes)

- A “Read Error” message indicates that the CRC on the disk did not match the CRC value that is recomputed by the drive hardware after the block is read.

- CRC can be reverse engineered to produced a predetermined value.

Validation of Evidence

Hash Message Digest 5 (RSAMD5)

Mathematical Algorithm that takes as input a message of arbitrary length and produces as output a 128-bit (16-byte) “digital fingerprint” or “message digest” of the input.

It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The odds of two different files having the same hash value is approximately 2^128 or 1x10^38.

Originally generated for digital signature applications, such as compressing large files before encryption and subsequent transmission.

Forensic Tools

Linux FREE

Coroner’s Toolkit Self contained Linux OS on bootable CD

Penguin Sleuth Kit Intuitive browser based tools

Knoppix

Windows $700 - $3000 per user

EnCase

Forensic Toolkit

Dongle Controlled

Digital Detective

Training Intensive and Expensive

WetStone

Examination Process

View Known Images.

Keyword Text String Searches.

Unallocated Graphic File Header Searches

Searching Email Files.

Restoring Programs and Applications to Working Drive and Navigating in the Suspects Environment.

Possible evidence image restoration to another drive.

Evidentiary Data

Data of Evidentiary Value and/or Investigative Interest are Extracted to a Folder on a Forensic Fixed Disk.

Data is labeled according to category and referred to in the Forensic Report.

Extracted Data is eventually cut to an autorun CD that allows a very functional and easy to use case layout.

Court Testimony

Expert Computer Forensic Testimony is relatively new to the Judicial System.

So far Law Enforcement has had a good handle on dealing with court testimony.

Just as in Biological Forensics, the Judge can qualify Computer Forensic Examiners as Computer Experts.

MSP Contact Information

Maryland State Police
Information Technology Bureau
Technical Investigation Division
Computer Forensic Laboratory
7155-C Columbia Gateway Drive
Columbia, Maryland 21046
Lt. Barry Leese, Commander
Sgt. David Heslep, TAS Supervisor

410-290-1620 - Voice
410-290-1831 - Fax

Break Time

Please take a
10 minute break!

Question and Answer

Q&A

This time is designed to provide an open forum of discussion.